

Rapport de l'exercice

Introduction

Ce projet a pour objectif la mise en pratique des principes de "Security by Design" à travers la création d'un formulaire de contact sécurisé en environnement local. Il vise à protéger les données utilisateurs contre diverses attaques connues (XSS, CSRF, interception de données, brute-force) tout en respectant les bonnes pratiques de gestion des mots de passe et de cookies. Le travail a été réalisé en utilisant Node.js, Express et plusieurs outils de sécurité tels que Helmet, bcrypt, et Google reCAPTCHA.

1. Développement et sécurisation du formulaire

Le développement du projet a été guidé par une démarche méthodique visant à répondre à chaque exigence du cahier des charges. L'objectif était de construire un système sécurisé dès l'architecture de base, tout en respectant les standards modernes du développement web sécurisé.

- La première étape a été l'organisation du dossier de travail. Une arborescence claire a été définie :

src/ contient le serveur Node.js (Express).

public/ regroupe les fichiers frontend : HTML, CSS, JS.

logs/ sert à consigner les accès et erreurs.

config/ssl/ stocke les certificats SSL générés localement.

Cette structure permet une bonne séparation des responsabilités et favorise la maintenabilité du projet. Un formulaire HTML (index.html) permet à l'utilisateur de saisir son nom, son adresse e-mail et un message. Ce formulaire est enrichi par :

- Une validation JavaScript côté client (regex pour l'e-mail, champs obligatoires).
- L'intégration de Google reCAPTCHA v2, utilisé pour éviter les soumissions automatisées.

2. Mise en place du serveur sécurisé

Le serveur a été développé avec Express.js et configuré pour fonctionner uniquement en HTTPS grâce à un certificat SSL auto-signé. Le code serveur (server.js) implémente deux fonctionnalités clés :

- La connexion via un formulaire d'authentification sécurisé.
- La réception, vérification et traitement des messages utilisateur.

- Des middlewares sont utilisés pour renforcer la sécurité :
- helmet applique automatiquement plusieurs en-têtes HTTP de protection (HSTS, CSP, XSS protection).
- express-session gère les sessions utilisateur avec des cookies sécurisés (HttpOnly, Secure).
- bcrypt sert à hacher le mot de passe de l'utilisateur démonstration.

a) Chiffrement et traitement des données

Les données du formulaire sont chiffrées avec l'algorithme AES-256-CBC. Cela garantit la confidentialité même en cas d'accès non autorisé au fichier messages.json. Le chiffrement s'applique sur les champs nom, email, et message.

b) Vérification côté serveur

Chaque envoi de formulaire est soumis à une double vérification pour garantir qu'il ne provient ni d'un bot ni d'un utilisateur non autorisé :

- Vérification du reCAPTCHA : lorsque l'utilisateur soumet le formulaire, un token g-recaptcha-response est automatiquement généré par Google reCAPTCHA. Ce token est envoyé au serveur avec les autres données du formulaire. Le serveur l'envoie ensuite à l'API de vérification de Google en fournissant aussi une clé secrète. Si la réponse confirme que le token est valide et récent, la requête peut continuer ; sinon, elle est bloquée.
- Contrôle de session : le serveur vérifie également que l'utilisateur a été authentifié au préalable (c'est-à-dire qu'il a une session active). Cela se fait grâce à la variable req.session.authenticated, définie uniquement après une connexion réussie. Si cette variable n'est pas présente ou fausse, la soumission du formulaire est refusée et l'utilisateur est redirigé vers la page de connexion.

c) Journalisation des activités

Un système de journalisation personnalisé a été mis en place. Les requêtes sont enregistrées dans logs/access.log, tandis que les erreurs (ex : échec d'authentification, captcha invalide) sont consignées dans logs/error.log. Cette traçabilité renforce la détection d'incidents et l'audit de sécurité.

d) Configuration HTTPS

Le certificat SSL a été généré en local avec OpenSSL. Le serveur Express est configuré pour utiliser ces fichiers (localhost.key, localhost.crt) et rediriger toute tentative de connexion HTTP vers HTTPS. Cela permet d'assurer une communication chiffrée de bout en bout entre l'utilisateur et le serveur.


3. Vérification de la sécurité

Plusieurs tests ont été menés pour évaluer la robustesse du système :

a) Test SSL Labs

Le serveur local a été exposé via Ngrok pour permettre l'analyse de sécurité via SSL Labs :

<https://4ada-2a02-842b-87bc-ca01-a9c6-afd-5da8-e39a.ngrok-free.app>

 Qualys SSL Labs			
Home Projects Qualys Free Trial Contact			
You are here: Home > Projects > SSL Server Test > 4ada-2a02-842b-87bc-ca01-a9c6-afd-5da8-e39a.ngrok-free.app			
SSL Report: 4ada-2a02-842b-87bc-ca01-a9c6-afd-5da8-e39a.ngrok-free.app			
Assessed on: Mon, 12 May 2025 21:13:01 UTC Hide Clear cache			
Scan Another >>			
	Server	Test time	Grade
1	3.14.182.203 ec2-3-14-182-203.us-east-2.compute.amazonaws.com Ready	Mon, 12 May 2025 21:03:51 UTC Duration: 106.425 sec	A
2	2600:1f16:d83:1200:0:0:6e:0 Ready	Mon, 12 May 2025 21:05:37 UTC Duration: 102.462 sec	A
3	2600:1f16:d83:1200:0:0:6e:3 Ready	Mon, 12 May 2025 21:07:19 UTC Duration: 109.23 sec	A
4	3.17.7.232 ec2-3-17-7-232.us-east-2.compute.amazonaws.com Ready	Mon, 12 May 2025 21:09:09 UTC Duration: 102.986 sec	A
5	3.134.125.175 ec2-3-134-125-175.us-east-2.compute.amazonaws.com Ready	Mon, 12 May 2025 21:10:52 UTC Duration: 81.415 sec	A
6	2600:1f16:d83:1201:0:0:6e:1 Failed to communicate with the secure server	Mon, 12 May 2025 21:12:13 UTC Duration: 7.177 sec	-
7	3.134.39.220 ec2-3-134-39-220.us-east-2.compute.amazonaws.com	Mon, 12 May 2025 21:12:20 UTC Duration: 7.214 sec	-

Résultats :

L'outil d'analyse SSL Labs de Qualys a été utilisé pour vérifier la configuration TLS du serveur.

Résultats obtenus :

- 5 serveurs d'évaluation ont pu se connecter avec succès.
- Tous les 5 ont attribué la note maximale : A.
- Aucun protocole obsolète (TLS 1.0, 1.1) n'est activé.
- Les certificats sont reconnus comme valides et bien configurés (via wildcard Ngrok).
- Temps de réponse maîtrisés, absence de redirections multiples, et chiffrement robuste.

Cette évaluation démontre que la couche HTTPS est correctement mise en place et que la sécurité de transport est conforme aux standards actuels.

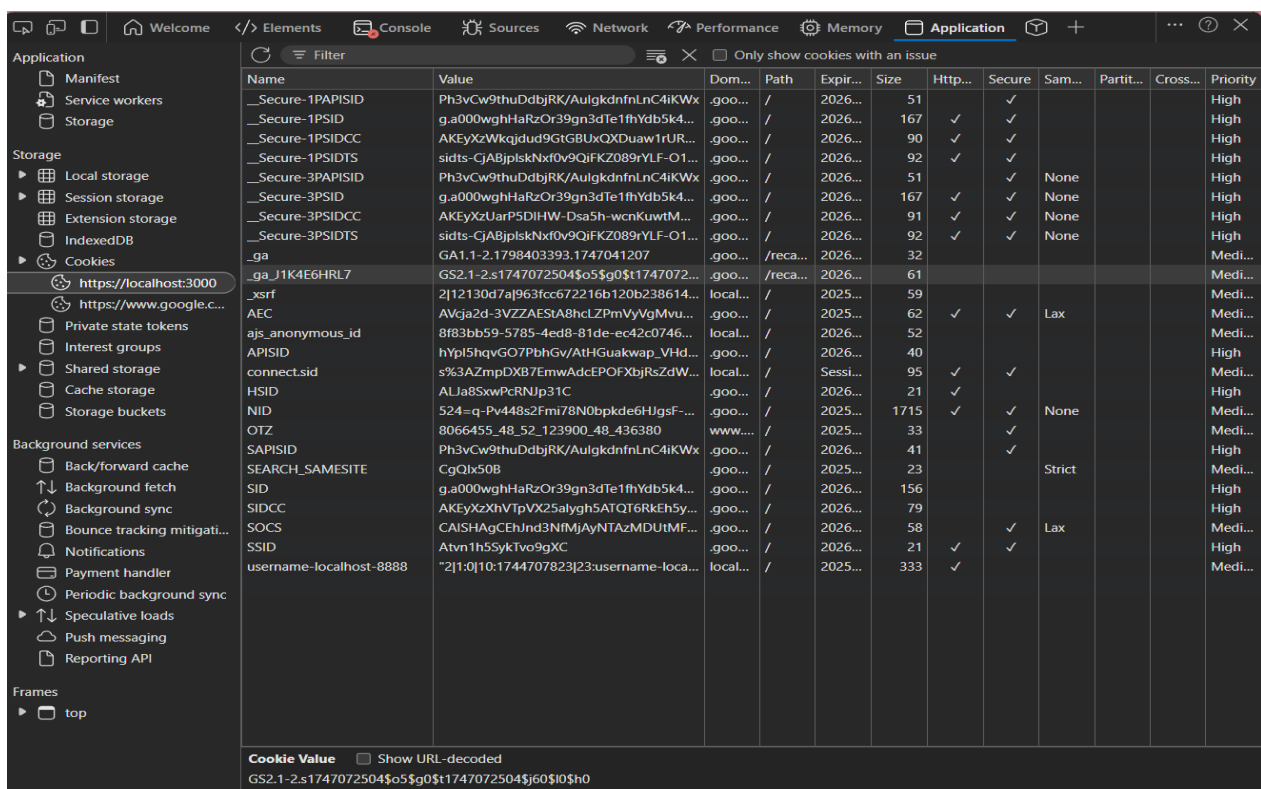
b) Vérification via DevTools

Les DevTools de Microsoft edge ont permis de vérifier que :

Les cookies sont bien marqués HttpOnly et Secure

Aucun script n'a pu être injecté via les champs du formulaire grâce au CSP

Une analyse a été effectuée à l'aide de l'onglet "Application" des DevTools du navigateur.



Name	Value	Dom...	Path	Expir...	Size	Http...	Secure	Sam...	Partit...	Cross...	Priority
__Secure-1PAPISID	Ph3vCw9thuDbjRK/AulgkdnfnLnC4iKWx...	.goo...	/	2026...	51		✓				High
__Secure-1PSID	g.a000wghHaRzOr39gn3dT1fhYdb5k4...	.goo...	/	2026...	167	✓	✓				High
__Secure-1PSIDCC	AKeyXzWkqjdud9GTGBUxQXDuaW1rUR...	.goo...	/	2026...	90	✓	✓				High
__Secure-1PSIDTS	sidts-CjABjplskNxf0v9QifKZ089rYLF-O1...	.goo...	/	2026...	92	✓	✓				High
__Secure-3PAPISID	Ph3vCw9thuDbjRK/AulgkdnfnLnC4iKWx...	.goo...	/	2026...	51		✓	None			High
__Secure-3PSID	g.a000wghHaRzOr39gn3dT1fhYdb5k4...	.goo...	/	2026...	167	✓	✓	None			High
__Secure-3PSIDCC	AKeyXzUarP5DIHW-Dsa5h-wcnKuwtM...	.goo...	/	2026...	91	✓	✓	None			High
__Secure-3PSIDTS	sidts-CjABjplskNxf0v9QifKZ089rYLF-O1...	.goo...	/	2026...	92	✓	✓	None			High
_ga	GA1.1-2.1798403393.1747041207	.goo...	/reca...	2026...	32						Medi...
_ga_J1K4E6HRL7	GS2.1-2.s1747072504\$05\$g0\$t1747072...	.goo...	/reca...	2026...	61						Medi...
_xsrf	2j12130d7a9p63fcc672216b120b238614...	local...	/	2025...	59						Medi...
AEC	AVcja2d-3VZZAESA8hcLZPmVvYgMvu...	.goo...	/	2025...	62	✓	✓	Lax			Medi...
ajs_anonymous_id	8f83bb59-5785-4ed8-81de-ec42c0746...	local...	/	2026...	52						Medi...
APISID	hYpI5hqvgO7PbhGv/AtHGuaKwap_VHd...	.goo...	/	2026...	40						High
connect.sid	s%3AZmpDXB7EmwAdcEPOFXbjRsZdW...	local...	/	Sessi...	95		✓	✓			Medi...
HSID	ALJa8SxwPcRNjp31C	.goo...	/	2026...	21	✓	✓				High
NID	524=q-Pv448s2fmi78N0bpkde6HJgsf-	.goo...	/	2025...	1715	✓	✓	None			Medi...
OTZ	8066455_48_52_123900_48_436380	www...	/	2025...	33		✓				Medi...
SAPISID	Ph3vCw9thuDbjRK/AulgkdnfnLnC4iKWx...	.goo...	/	2026...	41		✓				High
SEARCH_SAMESITE	CgQlx50B	.goo...	/	2025...	23			Strict			Medi...
SID	g.a000wghHaRzOr39gn3dT1fhYdb5k4...	.goo...	/	2026...	156						High
SIDCC	AKeyXzXhVTpVX25alygh5ATQT6RkEh5y...	.goo...	/	2026...	79						High
SOCS	CAISHAgCEhJnd3NfMjAyNTAzMdUIMF...	.goo...	/	2026...	58		✓	Lax			Medi...
SSID	Atvn1h5SykTvo9gXC	.goo...	/	2026...	21	✓	✓				High
username-localhost-8888	*2j10j10:1744707823j23:username-loca...	local...	/	2025...	333	✓					Medi...

Cookie Value ☐ Show URL-decoded
GS2.1-2.s1747072504\$05\$g0\$t1747072504\$5j60\$IO\$h0

- Le cookie de session `connect.sid`, utilisé pour gérer les connexions utilisateurs, est bien configuré avec les attributs `HttpOnly` et `Secure`.

- Ces attributs empêchent le vol de session via des scripts injectés (XSS) ou via une transmission non sécurisée.

- L'attribut `SameSite` est également visible sur certains cookies, renforçant la protection contre les attaques CSRF.

Cette configuration respecte les bonnes pratiques en matière de gestion des cookies de session.

c) Vérifier la résistance aux attaques XSS

Nous avons injecté des balises `<script>` « `<script>alert("XSS")</script>` » dans les champs de saisie. Le site a chiffré ces entrées et les a stockées dans `messages.json` sans les exécuter. Lors de l’affichage, les balises étaient échappées, confirmant une protection efficace contre les XSS stockés.

Conclusion

À travers ce projet, une application web locale a été conçue selon les principes de la "Security by Design", en intégrant la sécurité dès les premières lignes de code. Chaque aspect critique — de la protection des données à la sécurisation des connexions — a été pris en compte.

L’ensemble des mécanismes mis en place (HTTPS, Helmet, reCAPTCHA, validation, chiffrement, journalisation) permet d'assurer une sécurité robuste adaptée à un contexte réel. Le projet est pleinement conforme aux exigences du cahier des charges et constitue une base solide pour toute extension future en environnement de production.